IN THE COURT OF COMMON PLEAS
HAMILTON COUNTY, OHIO

JOHN DOE, on behalf of himself and all others similarly situated, c/o Markovits, Stock & DeMarco, LLC 119 East Court Street, Suite 530 Cincinnati, Ohio 45202 Plaintiff, vs. **THE CHRIST HOSPITAL** 2139 Auburn Avenue Cincinnati, Ohio 45219 Defendant.	CASE NO. A2204749 JUDGE **CLASS ACTION COMPLAINT** MOTION FOR TEMPORARY RESTRAINING ORDER AND AFFIDAVITS IN SUPPORT FILED JURY DEMAND

Plaintiff John Doe ("Plaintiff"),[1] by undersigned counsel, and for his Complaint avers as follows, upon personal knowledge as to his own actions, upon the investigation of his counsel, and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. Plaintiff, individually and on behalf of all others similarly situated, brings this action for damages and injunctive relief against The Christ Hospital ("Christ Hospital" or "Defendant") for Defendant's systematic, ongoing practice of unlawfully disclosing Plaintiff's and proposed Class Members' personal, sensitive medical information to a third-party without notice or consent.

2. The Christ Hospital has a duty to its patients and the public to keep personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") confidential. Defendant is prohibited from disclosing Private Information to third parties without knowledge, consent, or authorization. Despite this clear prohibition under the law,

[1] Plaintiff respectfully intends to proceed under a pseudonym in public filings so as not to compound the loss of privacy already suffered. Plaintiff will file a motion to proceed under a pseudonym after conferring with Defendant's counsel to determine if the motion will be opposed. Plaintiff does not object to sharing his identity with the Court or opposing counsel.

Defendant does just that.

3. Defendant maintains a website at www.thechristhospital.com (the "Website"). Through the Website, patients and other members of the public can search for specific doctors or medical providers within the Christ Hospital network, which allows users to filter by location or medical specialty. From there, individuals can schedule appointments and learn more about the specific services provided. The Website also allows returning patients to access a patient portal ("MyChart"), wherein patients can view medical records and test results, schedule appointments, or communicate with their doctors.

4. Defendant expressly and impliedly promises Plaintiff and its other patients that it will maintain the privacy and confidentiality of communications that patients exchange with Christ Hospital on its Website and through MyChart.

5. Plaintiff, Class Members, and Ohio consumers expect that communications and interactions with Christ Hospital from which Private Information can be viewed or inferred will be confidential and not shared with third parties. This is based on the nature of service provided by Defendant, along with Defendant's express and implied promises, statutes, rules, and industry standards and customs.

6. Contrary to Defendant's representations, consumer's reasonable expectations, and Ohio law, when an individual interacts with Defendant through the Website, a tracking product known as a "Facebook Pixel," which Defendant embeds on its website, discloses information about that interaction to third parties, including Meta Platforms, Inc., d/b/a Meta ("Meta" or "Facebook"), the developer of the Facebook Pixel. The information communicated to Meta by Defendant's embedded code following interactions with the Website is sufficient for Meta and other third parties to infer or plainly view Private Information, such as the identity of the person interacting with the Website, their IP address, and the type of illness or injury that they are seeking

treatment for. This information is then used to more efficiently target patients with advertisements.

7. Defendant does not inform its patients or the public that it makes unauthorized disclosures of Private Information to third parties like Meta.

PARTIES

8. Plaintiff John Doe is a natural person and citizen of Ohio, residing in Hamilton County, Ohio. He is a patient of Christ Hospital and maintains an active Facebook account.

9. Defendant The Christ Hospital is a 501(c)(3) non-profit corporation organized under, and governed by, Ohio law. Defendant operates a health care network comprising two medical centers, 1,200 physicians, and 6,500 employees, across more than 100 locations in the Greater Cincinnati area.[2]

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under R.C. 2305.01 and R.C. 1345.04.

11. This Court has personal jurisdiction over Defendant because it is incorporated under Ohio law, its principal place of business is in this State, and the acts and omissions giving rise to Plaintiff's claims occurred in this State.

12. Venue is proper in Hamilton County under Civ.R. 3(C)(2) because Defendant's principal place of business is in this county.

BACKGROUND

13. The Website contains a Facebook tracking pixel that secretly enables the unauthorized transmission and disclosure of Plaintiff's and Class Members' Private Information to Facebook.

[2] https://www.thechristhospital.com/about-the-network (last visited: December 22, 2022).

14. A pixel is a piece of code that "tracks the people and [the] type of actions they take."[3] Pixels are routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Pixel data to improve and save costs on its marketing campaign, improve its data analytics, and attract new patients. In other words, Defendant implemented the Facebook Pixel to bolster its profits.

15. Operating as designed, Defendant's tracking Pixel allowed the Private Information that Plaintiff and Class Members submitted to Defendant to be unlawfully disclosed to Facebook.

16. For example, when Plaintiff or a Class Member accessed the Website hosting the Facebook Pixel, the Facebook software directed Plaintiff's or Class Members' browser to send a message to Facebook's servers. The information Defendant sent to Facebook included the Private Information that Plaintiff and Class Members submitted to the Website, including for example, the type and date of a medical appointment and physician. Such Private Information would allow a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific patient was being treated for specific types of medical conditions such as cancer, psychiatric disorders, or sexually-transmitted diseases.

17. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on activity conducted on the Website.

18. Defendant regularly encourages Plaintiff and Class Members to use the digital tools on its Website to seek and receive healthcare services. Plaintiff and Class Members provided their

[3] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Nov. 14, 2022)

Private Information through the Website with the reasonable understanding that Defendant would secure and maintain any Private Information as confidential.

19. At all times that Plaintiff and Class Members visited and utilized the Website, they had a reasonable expectation of privacy in the Private Information collected, including that it would remain secure and protected and utilized only for medical purposes.

20. Defendant made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

21. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and medical information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

22. Defendant, however, violated and failed in its obligations and promises by utilizing the Facebook Pixel, described below, on its Website, knowing that such technology would transmit and share Plaintiff's and Class Members' Private Information with unauthorized third parties.

23. The exposed Private Information of Plaintiff and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting, or insurance companies utilizing the information to set insurance rates. Furthermore, third parties can often offer for sale the unencrypted, unredacted Private Information to criminals on the dark web for use in fraud and cyber-crimes.

24. While Defendant intentionally incorporated the tracking Pixel into its website, Defendant has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications via the Website with Facebook. As a result, Plaintiff and Class

Members were unaware that their Private Information were being surreptitiously transmitted to Facebook as they visited their healthcare provider's Website.

25. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiff and Class Members that this was happening; and (vi) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

26. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of their Private Information, and (v) the continued and ongoing risk of irreparable harm.

27. Plaintiff seeks to remedy these harms through claims for (i) breach of confidence, (ii) invasion of privacy – intrusion upon seclusion; (iii) breach of implied contract; (iv) unjust enrichment; (v) violations of the Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq.*; and (vi) violations of the Ohio Wiretap Act, R.C. 2933.52.

Defendant Improperly Disclosed Plaintiff's and Class Members' Private Information

28. Defendant employs its Website to connect Plaintiff and Class Members to Defendant's digital healthcare platform with the goal of increasing profitability.

29. To accomplish this, upon information and belief, Defendant utilized Facebook

advertisements and intentionally installed the Pixel on its website. The Pixel is a piece of code that Defendant commonly used to secretly track patients' activities by recording the information they both accessed and communicated on Defendant's Website.

30. Through seeking and using Defendant's services as a medical provider, and utilizing the Website, Plaintiff's and Class Members' Private Information was intercepted in real time and then disseminated to Facebook, and potentially to other third parties, via the Pixel that Defendant secretly installed on its website.

31. Plaintiff and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook or that Defendant was tracking their use of the Website, including the information they accessed and their logging into the MyChart portal, and disclosing them to Facebook, when they entered highly sensitive information on Defendant's Website.

32. Defendant did not disclose to or warn Plaintiff or Class Members that Defendant used Plaintiff's and Class Members' confidential electronic medical communications for marketing purposes.

33. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information, particularly not beyond the limits of Defendant's promises expressed in advance in its published policies.

34. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiff's and Class Members' status as medical patients;

b. Plaintiff's and Class Members' use of the MyChart portal, thus confirming their status as patients of Defendant in particular;

c. Plaintiff's and Class Members' communications with Defendant through

its Website; and

d. Plaintiff's and Class Members' searches for information on specific medical conditions and treatments, location of treatment facilities, and medical providers of specific types.

35. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (i) implemented technology (i.e., the Facebook Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (ii) disclosed patients' protected information to Facebook—an unauthorized third party; and (iii) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

Web Page Markup and Source Code

36. Web browsers are software applications that allow consumers to exchange electronic communications over the internet.

37. Every website is hosted by a computer "server" through which the entity in charge of the website exchanges communications with Internet users via a "client device," such as a computer, tablet, or smart phone, through the client device's web browser.

38. Each exchange of electronic communication over the internet consists of an HTTP Request from a client device and an HTTP Response from a server. When a user types a URL into a web browser, for instance, that URL is sent as an HTTP Request to the server corresponding to the web address, and the server returns an HTTP Response that consists of the web page to display in the client device's web browser.

39. In addition to specifying a URL, HTTP Requests can send data to the host server, including users' cookies. Cookies are text files stored on client devices to record data, often containing sensitive, personally identifying information.

40. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

41. A web page consists primarily of "Markup" and "Source Code." The Markup of a web page comprises the visible portion of that web page. Markup is displayed by a web browser in the form of words, paragraphs, images, and videos on the screen. The Source Code of a web page is a set of instructions that commands the browser to take certain actions, either when the web page first loads or when a specified event triggers the code.

42. For instance, typing "https://www.thechristhospital.com/physician" into a browser sends an HTTP Request to Defendant's Website, which returns an HTTP Response in the form of a web page displaying the following:

43. Source code is not visible on the client device's screen, but it may change the Markup of a web page, thereby changing what is displayed on the client device's screen. Source code may also execute a host of other programmatic instructions, including commanding a web browser to send data transmissions in the form of HTTP Requests to the website's server or, as is

the case with Defendant's Website, to third parties via pixels.

44. For instance, Defendant's web page pictured above includes code that sends HTTP Requests directly to Facebook, including patients' Private Information. One such HTTP Request sent without patients' knowledge is as follows:

method: POST
url: https://www.facebook.com/tr/
httpVersion: http/1.1
headers:
[{'name': ':authority', 'value': 'www.facebook.com'}, {'name': ':method', 'value': 'POST'}, {'name': ':path', 'value': '/tr/?id=7151rbyksh541ipfbfrs7o96lqkib4zu'}, {'name': ':scheme', 'value': 'https'}, {'name': 'accept', 'value': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9'}, {'name': 'accept-encoding', 'value': 'gzip, deflate, br'}, {'name': 'accept-language', 'value': 'en-US,en;q=0.9'}, {'name': 'cache-control', 'value': 'max-age=0'}, {'name': 'content-length', 'value': '4116'}, {'name': 'content-type', 'value': 'application/x-www-form-urlencoded'}, {'name': 'cookie', 'value': 'sb=ewMyYqaTMtIs-sx4Y6lmlkwj; datr=ewMyYtQzmmMstZpZmB22bB2u; locale=en_US; c_user=[redacted]; xs=32%3AKXXdrGmNyj5DlA%3A2%3A1670391700%3A-1%3A5353%3A%3AAcWAt6T2cS1Jzf86Q2hvwWyPRn4f2EWdDdTWOXQm3Q; fr=0poLy6y7Px5iLs1z9.AWVcoTT_jfOHJWVfksaCCSrND4I.BjkbLi.f8.AAA.0.0.BjkbLi.AWU1Ef1rFuc'}, {'name': 'origin', 'value': 'https://www.thechristhospital.com'}, {'name': 'referer', 'value': 'https://www.thechristhospital.com/'}, {'name': 'sec-ch-ua', 'value': '"Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"'}, {'name': 'sec-ch-ua-mobile', 'value': '?0'}, {'name': 'sec-ch-ua-platform', 'value': '"Windows"'}, {'name': 'sec-fetch-dest', 'value': 'iframe'}, {'name': 'sec-fetch-mode', 'value': 'navigate'}, {'name': 'sec-fetch-site', 'value': 'cross-site'}, {'name': 'sec-fetch-user', 'value': '?1'}, {'name': 'upgrade-insecure-requests', 'value': '1'}, {'name': 'user-agent', 'value': 'Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36'}]
queryString:
[]
cookies:
[{'name': 'sb', 'value': 'ewMyYqaTMtIs-sx4Y6lmlkwj', 'path': '/', 'domain': '.facebook.com', 'expires': '2024-01-11T05:41:36.444Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}, {'name': 'datr', 'value': 'ewMyYtQzmmMstZpZmB22bB2u', 'path': '/', 'domain': '.facebook.com', 'expires': '2024-03-15T03:34:14.128Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}, {'name': 'locale', 'value': 'en_US', 'path': '/', 'domain': '.facebook.com', 'expires': '2022-12-14T05:40:31.231Z', 'httpOnly': False, 'secure': True, 'sameSite': 'None'}, {'name': 'c_user', 'value': '[redacted]', 'path': '/', 'domain': '.facebook.com', 'expires': '2023-12-08T09:48:17.695Z', 'httpOnly': False, 'secure': True, 'sameSite': 'None'}, {'name': 'xs', 'value': '32%3AKXXdrGmNyj5DlA%3A2%3A1670391700%3A-1%3A5353%3A%3AAcWAt6T2cS1Jzf86Q2hvwWyPRn4f2EWdDdTWOXQm3Q', 'path': '/', 'domain': '.facebook.com', 'expires': '2023-12-08T09:48:17.695Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}, {'name': 'fr', 'value': '0poLy6y7Px5iLs1z9.AWVcoTT_jfOHJWVfksaCCSrND4I.BjkbLi.f8.AAA.0.0.BjkbLi.AWU1Ef1rFuc', 'path': '/', 'domain': '.facebook.com', 'expires': '2023-03-08T09:48:16.695Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}]
headersSize: -1
bodySize: 4116
postData:

45. The above HTTP Request is a 'POST' Request, a kind of HTTP Request that includes data and requests that the host server accept that data. This particular POST Request is sending data to "https://facebook.com/tr/" and includes numerous cookies. Among these cookies is the patient's c_user id, an identifier that can be used to uniquely identify the patient by their Facebook account.

The Facebook Pixel

46. The reason Defendant's web page sends this Personal Information in an HTTP Request to Facebook is because Defendant secretly deployed the 'Facebook Pixel' on its website, in violation of its common law, contractual, statutory, and regulatory duties and obligations.

47. The Facebook Pixel is a marketing product provided by Meta in the form of a "piece of code," which Meta's customers (like Christ Hospital) then embed in the source code of the companies' web pages. According to Facebook, embedding its Pixel allowed the Defendant to "understand the effectiveness of [their] advertising and the actions [patients] take on [their] site."[4] It also allowed the Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, learn about the website, and decrease advertising and marketing costs.[5]

48. Most importantly, it allowed Defendant and Facebook to secretly track and intercept patients' communications on Defendant's Website. When patients visit Defendant's Website, unbeknownst to them, the web page displayed on the patient's browser includes the Facebook Pixel as embedded code (which is not visible to the patient). As shown above, this code is triggered as the patient interacts with the web page. Each time the Pixel is triggered, the code is executed and sends Personal Information from the client device directly to Facebook.

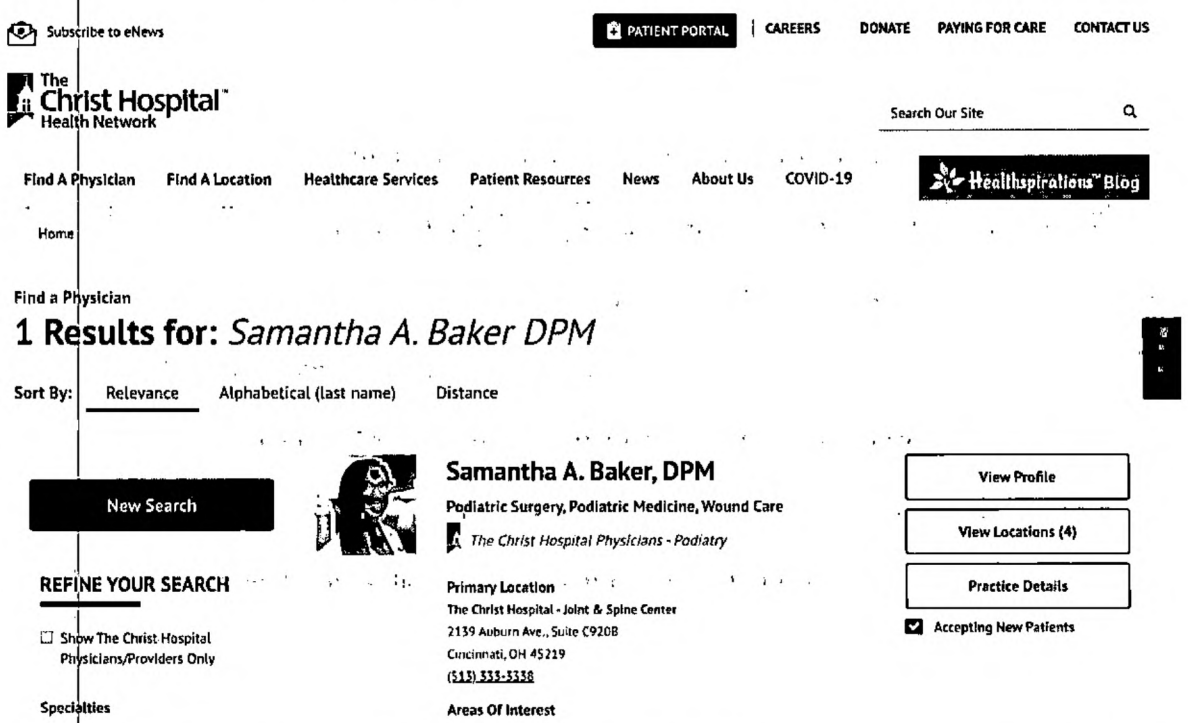
49. These pixels act like a physical wiretap on a phone, altering the structure of the communication device in a way that is not visible to the device's user. Like a physical tap, pixels do not appear to alter the function of the communication device on which they are installed. Instead, they wait until they are triggered by an event, at which time they effectively open a channel through which the website instructs the client device to funnel data about users and their actions to third parties through a hidden HTTP Request that is never shown to or agreed upon by the user.

---

[4] https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 14, 2022)

[5] *Id.*

50. For instance, from the "https://www.thechristhospital.com/physician" pictured above, the patient can enter in the name of a physician, "Samantha A. Baker DPM." In doing so, the patient's web browser sends an HTTP Request to Defendant's server with the URL "https://www.thechristhospital.com/physician-search-results?Type=providername&PhysicianID=%23000KG7B59&PhysicianName=Samantha%20A.%20Baker,%20DPM&ExactMatch=name". As expected, Defendant's server in turn sends an HTTP Response which displays the physician's information to the patient:



51. This is not the only HTTP Request Defendant's web page sends, however. In fact, at the very same time the web page is instructed to send an HTTP Request to Defendant requesting the specified doctor's information, the embedded Facebook Pixel acting as a tap is triggered, whereby Defendant's web page is also instructed to send an HTTP Request directly to Facebook notifying the social media giant of the patient's exact search:

method: GET
url: https://www.facebook.com/tr/?id=631586183931039&ev=PageView&dl=https://www.thechristhospital.com/physician-search-results?Type=_removed_&PhysicianID=_removed_&PhysicianName=Samantha+A.+Baker%2C+DPM&ExactMatch=name&_filteredParams=%7B%22unwantedParams%22%3A%5B%5D%2C%22sensitiveParams%22%3A%5B%22baaddf70fb5d432b8bd948ef91d6f910124a6d138edae4d5f000c4610ddc8eae%22%2C%2275622d2c4b480bffa55f0187fc11b769629a970b37a2394e42aaf6d3de93c5f5%22%5D%7D&rl=https://www.thechristhospital.com/physician?_filteredParams=%7B%22unwantedParams%22%3A%5B%5D%2C%22sensitiveParams%22%3A%5B%5D%7D&if=false&ts=1670496191110&sw=1366&sh=768&v=2.9.89&r=stable&ec=0&o=30&fbp=fb.1.1670496157951.955238516&it=1670496190958&coo=false&rqm=GET
httpVersion: http/1.1
headers:

[{'name': ':authority', 'value': 'www.facebook.com'}, {'name': ':method', 'value': 'GET'}, {'name': ':path', 'value': '/tr/?id=631586183931039&ev=PageView&dl=https%3A%2F%2Fwww.thechristhospital.com%2Fphysician-search-results%3FType%3D_removed_%26PhysicianID%3D_removed_%26PhysicianName%3DSamantha%2BA.%2BBaker%252C%2BDPM%26ExactMatch%3Dname%26_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522sensitiveParams%2522%253A%255B%2522baaddf70fb5d432b8bd948ef91d6f910124a6d138edae4d5f000c4610ddc8eae%2522%252C%252275622d2c4b480bffa55f0187fc11b769629a970b37a2394e42aaf6d3de93c5f5%2522%255D%257D&rl=https%3A%2F%2Fwww.thechristhospital.com%2Fphysician%3F_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522sensitiveParams%2522%253A%255B%255D%257D&if=false&ts=1670496191110&sw=1366&sh=768&v=2.9.89&r=stable&ec=0&o=30&fbp=fb.1.1670496157951.955238516&it=1670496190958&coo=false&rqm=GET&dt=f2u2wuenx7658756u3a1vxe7b1bp36xm'}, {'name': ':scheme', 'value': 'https'}, {'name': 'accept', 'value': 'image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8'}, {'name': 'accept-encoding', 'value': 'gzip, deflate, br'}, {'name': 'accept-language', 'value': 'en-US,en;q=0.9'}, {'name': 'cookie', 'value': 'sb=ewMyYqaTMtIs-sx4Y6lmlkwj; datr=ewMyYtQzmmMstZpZmB22bB2u; locale=en_US; c_user=100011152182075; xs=32%3AKXXdrGmNyj5D1A%3A2%3A1670391700%3A-1%3A5353%3A%3AAcWAt6T2cS1Jzf86Q2hvwWyPRn4f2EWdDdTWOXQm3Q; fr=0poLy6y7Px5iLs1z9.AWVcoTT_jfOHJWVfksaCCSrND4I.BjkbLi.f8.AAA.0.0.BjkbLi.AWU1Ef1rFuc'}, {'name': 'referer', 'value': 'https://www.thechristhospital.com/'}, {'name': 'sec-ch-ua', 'value': '"Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"'}, {'name': 'sec-ch-ua-mobile', 'value': '?0'}, {'name': 'sec-ch-ua-platform', 'value': '"Windows"'}, {'name': 'sec-fetch-dest', 'value': 'image'}, {'name': 'sec-fetch-mode', 'value': 'no-cors'}, {'name': 'sec-fetch-site', 'value': 'cross-site'}, {'name': 'user-agent', 'value': 'Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36'}]

queryString:

[{'name': 'id', 'value': '631586183931039'}, {'name': 'ev', 'value': 'PageView'}, {'name': 'dl', 'value': 'https%3A%2F%2Fwww.thechristhospital.com%2Fphysician-search-results%3FType%3D_removed_%26PhysicianID%3D_removed_%26PhysicianName%3DSamantha%2BA.%2BBaker%252C%2BDPM%26ExactMatch%3Dname%26_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522sensitiveParams%2522%253A%255B%2522baaddf70fb5d432b8bd948ef91d6f910124a6d138edae4d5f000c4610ddc8eae%2522%252C%252275622d2c4b480bffa55f0187fc11b769629a970b37a2394e42aaf6d3de93c5f5%2522%255D%257D'}, {'name': 'rl', 'value': 'https%3A%2F%2Fwww.thechristhospital.com%2Fphysician%3F_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522sensitiveParams%2522%253A%255B%255D%257D'}, {'name': 'if', 'value': 'false'}, {'name': 'ts', 'value': '1670496191110'}, {'name': 'sw', 'value': '1366'}, {'name': 'sh', 'value': '768'}, {'name': 'v', 'value': '2.9.89'}, {'name': 'r', 'value': 'stable'}, {'name': 'ec', 'value': '0'}, {'name': 'o', 'value': '30'}, {'name': 'fbp', 'value': 'fb.1.1670496157951.955238516'}, {'name': 'it', 'value': '1670496190958'}, {'name': 'coo', 'value': 'false'}, {'name': 'rqm', 'value': 'GET'}]

cookies:
[{'name': 'sb', 'value': 'ewMyYqaTMtIs-sx4Y6lmlkwj', 'path': '/', 'domain': '.facebook.com', 'expires': '2024-01-11T05:41:36.444Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}, {'name': 'datr', 'value': 'ewMyYtQzmmMstZpZmB22bB2u', 'path': '/', 'domain': '.facebook.com', 'expires': '2024-03-15T03:34:14.128Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}, {'name': 'locale', 'value': 'en_US', 'path': '/', 'domain': '.facebook.com', 'expires': '2022-12-14T05:40:31.231Z', 'httpOnly': False, 'secure': True, 'sameSite': 'None'}, {'name': 'c_user', 'value': '[redacted]', 'path': '/', 'domain': '.facebook.com', 'expires': '2023-12-08T09:48:17.695Z', 'httpOnly': False, 'secure': True, 'sameSite': 'None'}, {'name': 'xs', 'value': '32%3AKXXdrGmNyj5DIA%3A2%3A1670391700%3A-1%3A5353%3A%3AAcWAt6T2cS1Jzf86Q2hvwWyPRn4f2EWdDdTWOXQm3Q', 'path': '/', 'domain': '.facebook.com', 'expires': '2023-12-08T09:48:17.695Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}, {'name': 'fr', 'value': '0poLy6y7Px5iLs1z9.AWVcoTT_jfOHJWVfksaCCSrND4I.BjkbLi.f8.AAA.0.0.BjkbLi.AWU1Ef1rFuc', 'path': '/', 'domain': '.facebook.com', 'expires': '2023-03-08T09:48:16.695Z', 'httpOnly': True, 'secure': True, 'sameSite': 'None'}]
headersSize: -1
bodySize: 0

52. This HTTP Request is a GET Request, a kind of Request that includes data in the URL itself. In this case, the URL contains the exact name of the Physician included in the patient's search. This information, along with the patient's personally-identifying cookies, are sent directly to Facebook without the patient's knowledge or consent, and at the same time the information is being sent to Defendant's own server.

53. In this way, any information a patient enters into Christ Hospital's Website can be secretly transmitted to Facebook while it is also being transmitted to Defendant's own server.

54. The third parties to whom a website transmits data through pixels do not provide any substantive content relating to the user's communications with the owner of the Website. Instead, these third parties are typically procured to track user data and communications for marketing purposes. As discussed below, this is exactly the purpose of Defendant's unlawful sharing of data with Facebook.

55. Thus, without any knowledge, authorization, or action by a user, a website developer like Defendant can use its source code to commandeer the user's computing device, causing the device in this case to contemporaneously and invisibly re-direct the users' Private Information to third parties. Unbeknownst to patients like Plaintiff and the proposed Class,

Defendant Christ Hospital did just that with the help of Facebook.

Facebook's Platform and its Business Tools

56. Facebook operates the world's largest social media company. In 2021, Facebook generated $117 billion in revenue.[6] Roughly 97% of that came from selling advertising space.[7]

57. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, including IP addresses.

58. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code.

59. Facebook then sells advertising space by highlighting its ability to target users.[8] Facebook can target users so effectively because it surveils user activity both on and off its site.[9] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[10] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[11]

60. Indeed, Facebook utilizes the precise type of information disclosed by Defendant to identify, target, and market products and services to individuals.

---

[6] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022)

[7] *Id.*

[8] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited Nov. 14, 2022) .

[9] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 14, 2022).

[10] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 14, 2022).

[11] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited Nov. 14, 2022).

61. Advertisers can also build "Custom Audiences."[12] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[13] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[14]

62. Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools," including the Facebook Pixel.[15]

63. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[16] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

---

[12] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Nov. 14, 2022).

[13] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 14, 2022).

[14] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Nov. 14, 2022).

[15] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Nov. 14, 2022).

[16] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087 (last visited Nov. 14, 2022).

64. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[17] Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[18] Advertisers can even create their own tracking parameters by building a "custom event." [19]

65. One such Business Tool is the Facebook Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their website. the Facebook Pixel "tracks the people and type of actions they take."[20] When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret, transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's websites: Defendant's own code, and Facebook's embedded code.

66. An example illustrates the point. Plaintiff submitted information from which his

---

[17] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Nov. 14, 2022).

[18] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Nov. 14, 2022)

[19] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (last visited Nov. 14, 2022)

[20] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

identity, location, and need to visit a nearby urgent care location could be seen or inferred. This information could then be combined with other information in Facebook's possession, like his name, date of birth, and phone number, to more effectively target Plaintiff with advertisements or sell his data to third parties.

67. Because Defendant utilizes the Facebook Pixel, Facebook's embedded code, written in JavaScript, is included within the web pages hosted on Defendant's Website. This embedded code "listens" to activity on the client device, including scrolling, typing, and selecting options from drop-down menus. Each time the Pixel is triggered, it causes the browser to secretly duplicate the patients' communication with Defendant, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

68. Consequently, when Plaintiff and Class Members visited the Website and entered their Private Information to the Website, it was transmitted to Facebook, including, but not limited to, appointment type and date, physician selected, specific button/menu selections, content typed into free-text boxes, demographic information, email addresses, phone numbers, and emergency contact information. During the same transmissions, the website would also provide Facebook with the patient's Facebook ID, IP address and/or device ID or other the information they input into the Website, like their home address or phone number.

69. This is precisely the type of information that HIPAA and other applicable law requires healthcare providers to de-identify to protect the privacy of patients.[21]

70. The Plaintiff's and Class Members identities could be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying

---

[21] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Nov. 14, 2022).

information that was improperly disclosed.

71. The Facebook Pixel also intercepts and transmits information that patients type into search boxes, e.g., "do I have covid", and forms that request confidential information like patient contact information, medical histories, insurance and financial information, and Social Security numbers.

72. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

73. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

Defendant's Privacy Policies and Promises

74. Defendant's privacy policies represent to Plaintiff and Class Members that Defendant will keep Private Information private and confidential and they will only disclose Private Information under certain circumstances.[22] None of these circumstances apply here.

75. Defendant's Notice of Privacy Practices explains Defendant's legal duties with respect to Private Information, and the purposes for which Defendant can lawfully use and disclose Plaintiff's and Class Members' Private Information, as follows:

- As authorized by the patient;
- To provide healthcare treatment;

[22]https://www.thechristhospital.com/patient-resources/privacy (last visited: December 22, 2022).

- To obtain payment for services;
- For healthcare operations;
- To maintain a facility directory;
- To family and friends involved in patient care;
- To business associates involved with healthcare operations;
- For fundraising solicitations to the patient, unless the patient opts out;
- For marketing, and where third parties are involved, only with patient authorization, and with disclosure of any payment to Defendant from a third party;
- In the case of psychotherapy notes, under several specific circumstances that do not involve marketing or direct financial gain by Defendant;
- For sale of PHI, only with specific patient authorization and disclosure of payment to Defendant;
- For appointment reminders and information about health services;
- For health-related benefits and services;
- In the case of alcohol and drug-abuse records, only with authorization, court order, or for healthcare-realted purposes.
- For reporting of crimes;
- In the case of HIV/AIDS testing or diagnosis, with authorization or court order;
- For various purposes required by law, including reporting and preventing crime, promoting public health, for certain governmental oversight and reporting, and to coroners, medical examiners, & funeral directors;
- To an employer, when treatment has been provided at the employer's request;
- For organ, eye, or tissue donation purposes;
- In case of a serious threat to health and safety;
- For research with appropriate safeguards;
- For military purposes, in the case of service members;
- To national security and intelligence agencies and officials, for the protection of the President and specific others;
- For workers' compensation purposes;
- For emergency medical treatment purposes;
- To inform the patient about health-related benefits and services; and
- For law enforcement purposes, or in response to legal processes, but only when efforts have been made to inform the patient or obtain a protective order to avoid disclosure.

76. Defendant's privacy policy does not permit Defendant to intercept and disclose Plaintiff's and Class Members' Private Information to third parties, including Facebook, for marketing purposes, without their consent.

77. Defendant's Privacy Policy acknowledges Defendant is required by law to maintain the confidentiality of Plaintiff's and Class Members' Private Information, subject to the exceptions listed above.[23]

78. Defendant violated its own privacy policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

Defendant Violated Ohio's Protected Health Information statute and Related HIPAA Standards

79. Ohio has made its laws governing the use and disclosure of protected health information consistent with HIPAA. *See* R.C. 3798.01, *et seq.* Ohio law adopts the same definitions of "covered entity," "disclosure," "health care provider," "health information," "protected health information," "individually identifiable health information," and "use" as provided by the HIPAA Privacy Rule. *See* R.C. 3798.01.

80. Defendant is a "covered entity" within the meaning of R.C. 3798.01.

81. Under R.C. 3798.03(A)(2), a covered entity shall "Implement and maintain appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information in a manner consistent with 45 C.F.R. 164.530(c)."

82. Under R.C. 3798.04, a covered entity shall not do either of the following:

(A) Use or disclose protected health information without an authorization that is valid under 45 C.F.R. 164.508 and, if applicable, 42 C.F.R. part 2, except when the use or disclosure is required or permitted without such authorization by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations and, if applicable, 42 C.F.R. part 2;

(B) Use or disclose protected health information in a manner that is not consistent with 45 C.F.R. 164.502.

[23] *Id.*

83. Under this statute and the federal standards it incorporates, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization, nor sell such information without disclosing that the disclosure will involve remuneration to the provider.[24]

84. Guidance from the United States Department of Health and Human Services ("HHS") instructs healthcare providers that patient status alone is protected by HIPAA. In *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule*, HHS instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[25]

85. In its guidance entitled *Marketing*, HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients…to third parties without obtaining authorization from each person on the list.[26]

86. In addition, the HHS Office for Civil Rights (OCR) has issued a Bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, which

---

[24] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

[25] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf §1.1 (last visited Dec. 28, 2022).

[26] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf, at 1-2 (last visited Dec. 28, 2022).

highlights the duties of these regulated entities under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[27]

87. The Bulletin expressly provides that **"[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."**[28] (Emphasis in original.) This sentence has an endnote stating, "Regulated entities can use or disclose PHI, without an individual's written authorization, only as expressly permitted or required by the HIPAA Privacy Rule. *See* 45 CFR 164.502(a)."[29]

88. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Facebook Pixel without the required notice to, and written authorizations from, its patients, including Plaintiff and Class Members.

Defendant Violated Industry Standards

89. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

90. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

91. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)

92. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is

---

[27] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
[28] *Id.*, at ¶2.
[29] *Id.*, at fn. 8.

> confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

93. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…:(c) release patient information only in keeping ethics guidelines for confidentiality.

IP Addresses are Personally Identifiable Information

94. On information and belief, through the use of the Facebook Pixel on the Website, Defendant also disclosed and otherwise assisted Facebook with intercepting Plaintiff's and Class Members' IP addresses.

95. An IP address is a number that identifies the address of a device connected to the Internet.

96. IP addresses are used to identify and route communications on the Internet.

97. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

98. Facebook tracks every IP address ever associated with a Facebook user.

99. Google also tracks IP addresses associated with Internet users.

100. Facebook, Google, and other third-party marketing companies track IP addresses for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

101. Under HIPAA, an IP address is considered personally identifiable information:

HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2). HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

102. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

Defendant Was Enriched from the Use of the Pixel and the Unauthorized Disclosures

103. Defendant used the Facebook Pixel on the Website solely for marketing purposes, related to increasing its ultimate profitability.

104. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

105. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

106. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

107. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

Plaintiff's Experience

108. In October 2022, after suffering an injury, Plaintiff searched the internet for nearby urgent care locations, whereupon he came across the Website. From Defendant's home page, Plaintiff navigated the Website to confirm the phone number of an appropriate urgent care location. Plaintiff recalls visiting at least the following URLs when initially searching for an urgent care

location to treat his injury: https://www.thechristhospital.com/; https://www.thechristhospital.com/locations; and https://www.thechristhospital.com/locations-search-results?Type=Advanced Search&Location=45247.

109. Upon information and belief, Plaintiff's use of the Website disclosed to Meta and other third parties his location, IP address, and the fact that he was seeking emergency medical treatment at a nearby Christ Hospital urgent care location. Upon information and belief, Meta was further able to connect this information with Plaintiff's specific Facebook account, which he has maintained and actively used during the relevant time period.

110. Following his use of the Website, Plaintiff travelled to Defendant's urgent location, where he received medical care. Plaintiff was then referred to additional providers within the Christ Hospital network for follow up treatment. Thereafter, he visited the Website to access the Christ Hospital patient portal so that he could view his medical test results.

111. Plaintiff did not, and does not, consent to the disclosure of his Private Information by Defendant to third parties like Meta for commercial purposes.

112. Plaintiff has suffered injury from the invasion of his privacy.

113. Plaintiff has suffered injury from the diminished value of his PII.

114. As identified by the United States Department of Health and Human Services, Plaintiff and Class Members have suffered and continue to suffer various injuries due to the disclosure of their Personal Health Information ("PHI") because "an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment." Use of Online

Tracking Technologies by HIPAA Covered Entities and Business Associates, Dec. 1, 2022 (last accessed on Dec. 28, 2022 at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html).

CLASS ACTION ALLEGATIONS

115. Plaintiff brings this action on behalf of himself and all others similarly situated, in accordance with Civ.R. 23, and seeks certification of the following class (the "Class"):

> **All patients of The Christ Hospital who visited a website belonging to Christ Hospital (or one of its agents), and as a result, had their protected health information (as defined by R.C. 3798.01) transmitted to third parties without authorization during the relevant time period.**

116. The relevant time period is the largest amount of time permitted by law.

117. Plaintiff respectfully reserves the right to amend the class definition or create additional subclasses.

118. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals.

119. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information it maintained;

c. Whether Defendant's use and disclosure of Private Information complied

with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. Whether Defendant's policies and procedures were consistent with industry standards and customs;

e. Whether Defendant owed a duty to Class Members to maintain the confidentiality of their Private Information;

f. Whether Defendant breached its duty to Class Members to maintain the confidentiality of their Private Information;

g. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

h. Whether Defendant's conduct was negligent, reckless, and/or intentional;

i. Whether Defendant's acts, inactions, and practices complained of herein amount to an invasion of privacy under the law;

j. Whether Defendant breached implied or express contracts with Plaintiff and Class Members;

k. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members; and

l. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

120. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised by Defendant.

121. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

122. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

123. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

124. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

COUNT I
Breach of Confidence (*Biddle*)
(on behalf of Plaintiff and the Class)

125. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

126. Medical providers in Ohio have a duty to their patients to keep Private Information confidential and to not disclose Private Information to third parties without the patient's informed consent or other applicable legal privilege entitling them to do so.

127. Plaintiff and Class Members had reasonable expectations of privacy when interacting with Defendant through the Website, including communications made on the Website, in virtue of this well-known duty of confidentiality incumbent upon medical providers.

128. Contrary to its duty as a medical provider, Defendant deployed the Facebook Pixel to disclose and transmit Private Information to third parties, including Meta, without patient authorization or consent.

129. Defendant's breaches of confidence were committed negligently, recklessly, and/or intentionally.

130. As a direct and proximate cause of Defendant's unauthorized disclosures of patient Private Information, Plaintiff and Class members were damaged by Defendant's breach in an amount to be determined at trial.

COUNT II
Invasion of Privacy – Intrusion Upon Seclusion
(on behalf of Plaintiff and the Class)

131. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

132. The Private Information of Plaintiff and Class Members is private, confidential, and not intended to be shared with third parties absent authorization.

133. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

134. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

135. The unauthorized disclosure and/or acquisition by a third party of Plaintiff's and

Class Members' Private Information via the use of the Facebook Pixel by Defendant is highly offensive to a reasonable person.

136. Defendant's negligent, reckless, and intentional disclosure of Plaintiff's and Class Members' Private Information constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

137. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

138. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it incorporated the Facebook Pixel into its website because it knew the functionality and purpose of the Facebook Pixel.

139. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its website and encouraged patients to use that website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

140. As a proximate result of Defendant's acts and omissions, the Private Information of Plaintiff and the Class Members was disclosed to a third party without authorization, causing Plaintiff and the Class to suffer damages.

141. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, punitive damages, plus prejudgment interest, and costs.

142. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and still

in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

143. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

144. Plaintiff, on behalf of himself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT III
Breach of Implied Contract
(on behalf of Plaintiff and the Class)

145. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

146. When Plaintiff and Class Members provided their user data to Defendant in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

147. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

148. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

149. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to a third party, *i.e.*, Facebook.

150. As a direct and proximate result of Defendant's breaches of these implied contracts,

Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class Members would not have used Defendant's services, or would have paid substantially for these services, had they known their Private Information would be disclosed.

151. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT IV
Unjust Enrichment
(on behalf of Plaintiff and the Class)

152. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein. Notwithstanding, this claim is brought in the alternative to breach of implied contract.

153. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

154. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

155. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

156. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in Ohio for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and

unconscionable methods, acts, and trade practices alleged in this Complaint.

157. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT V

Violations of the Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq.*
(on behalf of Plaintiff individually and as a private attorney general)

158. Plaintiff repeats and re-alleges each and every paragraph in the Complaint as if fully set forth herein.

159. Plaintiff brings this claim for declaratory judgment and injunctive relief under the Consumer Sales Practices Act individually and in his capacity as a private attorney general under R.C. 1345.09(D).

160. Plaintiff is a consumer who engaged in a consumer transaction with Defendant when he reviewed the Website and provided Defendant with his Private Information for purposes of locating and receiving medical services.

161. Defendant is a supplier because it regularly supplies medical services to consumers like Plaintiff for personal and/or family purposes and uses the Private Information that it receives from its patients for commercial purposes.

162. Defendant knowingly discloses the Private Information of Plaintiff and other Ohio consumers for purposes of more effectively targeting them with advertisements. These disclosures allow third parties, such as Meta, to view or accurately infer the Private Information of Plaintiff and other Ohio consumers and then match this Private Information with their specific identities. This information can then be, and upon information and belief is, sold to and used by other third parties for commercial purposes.

163. The CSPA requires courts to "give due consideration and great weight to federal trade commission orders, trade regulation rules and guides, and the federal courts' interpretations of subsection 45 (a)(1) of the 'Federal Trade Commission Act,' 38 Stat. 717 (1914), 15 U.S.C.A. 41, as amended." R.C. 1345.02(C). The failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an unfair practice in violation of the Federal Trade Commission Act. *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 244-247 (3d Cir. 2015); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F.Supp.3d 1295, 1327-1328 (N.D. Ga. 2019).

164. Defendant did not simply fail to protect Private Information from cybercriminals like the defendants in *Equifax* and *Wyndham*. Instead, Defendant reprehensibly installed the Facebook Pixel on its website to disclose and profit from the Private Information of Ohio consumers without their knowledge or consent. This is unfair, deceptive, and unconscionable.

165. The failure to affirmatively disclose to its patients and website users that Private Information will be shared for commercial purposes with third parties (such as Meta) is a deceptive omission in violation of R.C. 1345.02(A).

166. In addition to its omissions, Defendant has made, and continues to make, affirmative misrepresentations in violation of R.C. 1345.02(A) concerning data security, including but not limited to the statements identified in its privacy policy.

167. Plaintiff and all other Ohio consumers continue to face a substantial risk of irreparable harm from Defendant's actions. Defendant is a major medical provider throughout the State of Ohio, with an especially large footprint in southwest Ohio, where Plaintiff resides. Depending on the type and severity of future illness or injury, Plaintiff may be required to seek Defendant's medical services. An injunction would serve the public interest because Plaintiff and

other Ohio residents should not be forced to choose between receiving necessary medical services and maintaining the confidentiality of their Private Information.

168. Plaintiff respectfully requests the Court enter judgment declaring that Defendant has violated R.C. 1345.02(A) and R.C. 1345.03(A) by engaging in the acts and practices described herein.

169. Plaintiff respectfully requests that the Court enjoin Defendant from continuing to commit the unfair and deceptive acts and practices described herein, and that it further award any other equitable relief deemed appropriate under R.C. 1345.09(D).

170. Plaintiff respectfully requests that the Court award attorneys' fees under R.C. 1345.09(F)(2) for Defendant's knowing violations of the CSPA.

COUNT VI

Interception and Disclosure of Electronic Communications in Violation of R.C. 2933.52

(on behalf of Plaintiff and the Class)

171. Plaintiff repeats and re-alleges each and every paragraph in the Complaint as if fully set forth herein.

172. Under R.C. 2933.65, a person whose electronic communications are intercepted, disclosed, or intentionally used in violation of R.C. 2933.51 to 2933.66 may bring a civil action to recover from the entity that engaged in the violation any relief that may be appropriate and that includes, but is not limited to, the following:

(1) The preliminary and other equitable or declaratory relief that is appropriate;

(2) Whichever of the following is greater:

> (a) Liquidated damages computed at a rate of two hundred dollars per day for each day of violation or liquidated damages of ten thousand dollars, whichever is greater;

(b) The sum of actual damages suffered by the plaintiff and the profits, if any, made as a result of the violation by the person or entity that engaged in the violation.

(3) Punitive damages, if appropriate;

(4) Reasonable attorney's fees and other litigation expenses that are reasonably incurred in bringing the civil action.

173. It is a violation of R.C. 2933.52(A)(1) for a person purposely to intercept, attempt to intercept, or procure another person to intercept or attempt to intercept an electronic communication.

174. It is a violation of R.C. 2933.52(A)(3) to use, or attempt to use, the contents of an electronic communication, knowing or having reason to know that the contents were obtained through the interception of an electronic communication in violation of R.C. 2933.51 to 2933.66.

175. The exceptions set forth in R.C. 2933(B)(4) are not applicable, even though Defendant was party to the communications, because the interceptions were for the purpose of committing tortious acts under the laws of this state.

176. Plaintiff and Class Members are individuals, and Defendant is a corporation, and all Parties to this action are therefore "persons" within the meaning of R.C. 2933.52(A), as defined by R.C. 2933.51(K) and R.C. 1.59(C).

177. Plaintiff's and Class Members' activities on the Website are electronic communications within the meaning of R.C. 2933.52, defined in R.C. 2933.51(N) as "a transfer of a sign, signal, writing, image, sound, datum, or intelligence of any nature that is transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system."

178. The Pixel as installed on the Website, taken together with the hardware devices and software used by Plaintiff and Class Members to access and use the Website, and the hardware devices and software of Defendant and Facebook used to host the Website and Pixel and to process and use the acquired communications, together with the hardware devices and software of any

third parties into whose possession the communications may have come through the actions of Defendant and/or Facebook, constitute individually and collectively interception devices within the meaning of R.C. 2933.52, defined in R.C. 2933.51(D) as "an electronic, mechanical, or other device or apparatus that can be used to intercept a wire, oral, or electronic communication".

179. Given that Defendant acquired the contents of Plaintiff's and Class Members' communications on the Website for tortious and otherwise injurious purposes, their acts in so acquiring those communications constitute interception within the meaning of R.C. 2933.52, defined in R.C. 2933.51(C) as "the … acquisition of the contents of any … electronic communication through the use of an interception device."

180. Given that Defendant acquired the contents of Plaintiff's and Class Members' communications on the Website for tortious and otherwise injurious purposes, and knew that Facebook would also use them for tortious and otherwise injurious purposes, Defendant's actions in transmitting those communications to Facebook by installing the Pixel on its Website constituted procuring another person to intercept electronic communications, in violation of R.C. 2933.52(A)(3).

181. As a result of Defendant's knowing and intentional interceptions of their electronic communications, Plaintiff and Class Members are entitled to preliminary and permanent injunctive relief, declaratory judgment, liquidated damages or actual damages in amounts to be proved under R.C. 2933.65(A)(2) but not less than Ten Thousand Dollars each, punitive damages, and their reasonable attorney's fees and litigation expenses.

COUNT VII
Right of Publicity, R.C. 2741.01, *et seq.*
(on behalf of Plaintiff and the Class)

182. Plaintiff repeats and re-alleges each and every paragraph in the Complaint as if fully set forth herein.

183. Plaintiff and Class Members have a property right in Private Information such as their name. Plaintiff's and Class Members' names have significant value in combination with their PHI and other Private Information.

184. Defendant used Plaintiff's and Class Members' personas, including their names, for commercial purposes in connection with advertising and performing medical services, as well as raising funds.

185. Under Ohio's right to publicity statute, an individual's "name" means the actual, assumed, or clearly identifiable name of or reference to a living or deceased individual that identifies the individual.

186. Plaintiff's and Class Members' unique FIDs allow Christ Hospital to match information about a person's interactions with Christ Hospital's website to a specific Facebook profile. By combining this data with information on a person's Facebook profile, including their name, Defendant is able to profit by more effectively marketing its services.

187. Defendant did not have Plaintiff's or Class Members' authorization (in the form required by the statute) to use their personas for a commercial purpose.

188. Defendant acted knowingly in using Plaintiff's and Class Members' personas for a commercial purpose without authorization.

189. Plaintiff and the Class seek statutory damages of $10,000 per class member, preliminary and permanent injunctive relief, reasonable attorneys' fees, costs, and expenses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and members of the putative class, requests judgment against Defendant and that the Court grant the following:

A. A temporary restraining order and/or preliminary injunction, as set forth in the Motion filed contemporaneously with this Complaint;

B. An Order certifying the Class and appointing Plaintiff and his Counsel to represent such Class;

C. Equitable and statutory relief permanently enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Private Information, and as may be necessary to protect the interests of Plaintiff, Class Members, and Ohio consumers;

D. An award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount exceeding $25,000 to be determined at trial, as allowable by law;

E. An award of punitive damages, as allowable by law;

F. An award of all attorneys' fees, costs, and litigation expenses allowed by law;

G. Pre- and post-judgment interest at the highest rate allowed by law on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

Dated: December 30, 2022

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
Dylan J. Gould (0097954)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
221 West Monroe Street, Suite 2100
Chicago, IL 60606
(847) 208-4585

gklinger@milberg.com

Joseph M. Lyon (0076050)
THE LYON LAW FIRM
2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Bryan L. Bleichner*
Philip J. Krzeski (0095713)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Counsel for Plaintiff & the Putative Class

**pro hac vice* forthcoming

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury as to all matters so triable herein.

/s/ Terence R. Coates
Terence R. Coates (0085579)

Counsel for Plaintiff and the Putative Class